UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

STUDENT DOE, on behalf of herself and all others similarly situated, Plaintiff, v. THE UNIVERSITY OF MICHIGAN BOARD OF REGENTS, KEFFER DEVELOPMENT SERVICES, LLC, and MATTHEW WEISS, Defendants.	CASE NO. 2:25-cv-10999 CLASS ACTION COMPLAINT DEMAND FOR A JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Student Doe ("Plaintiff"), individually and on behalf of all others similarly situated, brings this consolidated class action complaint against Defendants The University of Michigan Board of Regents ("University of Michigan"), Keefer Development Services, LLC ("Keefer"), and Matthew Weiss (collectively, "Defendants"), and alleges, upon personal knowledge as to her own actions and experiences and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Student Doe brings this class action against Defendants University of Michigan and Keefer for the failure to properly secure the highly sensitive personally identifiable information ("PII") and protected health information ("PHI") of more than 150,000 student athletes, including herself, which was targeted, accessed, and exfiltrated by former University of Michigan quarterback coach and sexual predator Matthew Weiss, over the course of nearly a decade.

2. Between approximately 2015 and January 2023, University of Michigan's Coach Weiss, gained unauthorized access to student athlete databases of more than 100 colleges and

universities that were maintained by Keffer, a third-party vendor contracted by the University of Michigan.

3. After gaining access to these databases, Defendant Weiss downloaded the PII and PHI of more than 150,000 athletes.

4. Then, using the information that he obtained from the student athlete databases and his own internet research, University of Michigan's Coach Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 target athletes. Defendant Weiss also illegally obtained access to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities across the country. Once Weiss obtained access to these accounts, he downloaded personal, intimate digital photographs and videos that were never intended to be shared beyond intimate partners.

5. University of Michigan's Coach Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics.

6. Through this scheme, unknown to account holders, Defendant Weiss downloaded personal, intimate digital photographs and videos.

7. The "Data Breach"—the exfiltration of the PII and PHI of over 150,000 students from the athletic databases Keefer maintained, and the targeted exfiltration of intimate, personal, digital photographs and videos of 3,300 students and athletes[1]—continued for nearly a decade because the University of Michigan and Keffer failed to prevent, detect, or stop University of Michigan's Coach Weiss from accessing those databases without and in excess of authorization.

[1] These intimate digital photographs and videos, together with the PII and PHI exposed in the Data Breach, are referred to herein as "Private Information."

8. In March 2025, University of Michigan's Coach Weiss was charged in a 24-count indictment alleging 14 counts of unauthorized access to computers and 10 counts of aggravated identity theft, by the U.S. Attorney for the Eastern District of Michigan, for Weiss's perpetration of the Data Breach.

9. This prolific and egregious Data Breach was entirely preventable by the University of Michigan and Keffer. As noted in a criminal complaint filed by the U.S. Attorney in the Eastern District of Michigan, Defendant Weiss breached the University of Michigan's and Keffer's database systems by exploiting passwords and other vulnerabilities in the University of Michigan's and Keffer's systems and authentication processes. On information and belief, neither the University of Michigan nor Keffer required that its employees or students implement safeguards like multi-factor authentication to access accounts, a standard practice for all entities collecting PII, especially medical data and PHI.

10. The Data Breach was a direct result of the University of Michigan's and Keefer's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' PII and PHI, and the University of Michigan's failure to reasonably oversee its employees, leaving the most sensitive and personal information of students, like Student Doe, vulnerable to exploitation by malicious predators like Defendant Weiss.

11. Student Doe brings this action on behalf of all persons whose Private Information was compromised as a result of the University of Michigan's and Keefer's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of the University of Michigan's and Keefer's inadequate information security practices; and (iii) effectively secure its network and database systems containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and

incidents.

12. All three Defendants disregarded the rights of Student Doe and Class Members. The University of Michigan and Keefer intentionally, willfully, recklessly, and/or negligently failed to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failed to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failed to take standard and reasonably available steps to prevent the Data Breach; failed to properly train their staff and employees on proper security measures; failed to provide Student Doe and the class prompt notice of the Data Breach; and, in the case of the University of Michigan, failed to reasonably and adequately supervise its employees, including Defendant Weiss.

13. The University of Michigan's and Keefer's conduct amounts to a violation of the duties they owed to Student Doe under common law tort claims and state and federal statutory law, rendering them liable to Student Doe and the class for the harms caused by this egregious and preventable invasion of privacy. Defendant Weiss is equally liable for the harms inflicted on Student Doe and the class by his intentional hacking and exfiltration of their Private Information under tort and statutory law.

14. Student Doe and the class suffered injury as a result of Defendants' conduct. These injuries included: invasion and loss of privacy, loss of dignity, humiliation, embarrassment, and severe emotional distress.

15. Student Doe seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Student Doe seeks remedies including, but not limited to, compensatory damages, nominal damages, punitive damages, and reimbursement of out-of-pocket costs.

17. Student Doe also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the putative class.

PARTIES

18. Plaintiff Student Doe is a resident and citizen of Arkansas and was a student athlete at Grambling State University. On or about March 26, 2025, Student Doe received notice from the United States Department of Justice Victim Notification System that she was identified as a victim or potential victim in the criminal case against University of Michigan's Coach Weiss: *United States v. Defendant(s) Matthew Weiss*.[2]

19. Defendant University of Michigan is a public research university in Ann Arbor, Michigan. The University was established on August 26, 1817, in Ann Arbor, Michigan. The University of Michigan Board of Regents is the entity that governs the University of Michigan. Mich. Comp. Laws §§ 390.3 and 390.4.

20. Defendant Matthew Weiss is an individual and citizen of Michigan. On March 20, 2025, Defendant Weiss was indicted on 24 counts of unauthorized access to computers and aggravated identity theft by the U.S. Attorney for the Eastern District of Michigan.

21. Defendant, Keffer Development Services, LLC, is a technology vendor operating the electronic medical record system, which contained the PII and PHI of Plaintiff and class members. Keffer is headquartered in Grove City, Pennsylvania.

JURISDICTION AND VENUE

22. The Court has subject-matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class;

[2] Student Doe's Notice of Data Breach, attached herein as Exhibit A.

and at least one member of the class, including Plaintiff, is a citizen of a state different from *any* Defendant.

23. This Court also has jurisdiction under 28 USC §§ 1331 and 1367 because Plaintiff alleges a claim under the Computer Fraud and Abuse Act, Stored Communications Act, 18 U.S.C. § 2701(a) *et seq*., and 42 U.S.C. §1983, and supplemental jurisdiction over additional related claims under 28 U.S.C. § 1367(a).

24. The Court has personal jurisdiction over Defendants named in this action because Defendant University of Michigan is located in and created under the laws of the state of Michigan, Defendant Weiss is a citizen of the state of Michigan, and Defendant Keffer directs business at the state of Michigan, conducts substantial business in Michigan, and has availed itself of the protections of Michigan state law. The conduct by Defendant Keffer which gives rise to the claims against Defendant Keffer in this Complaint was directed at and occurred in Michigan.

25. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant Keffer and its Athletic Trainer System Software

26. Defendant Keffer is a software development vendor that developed an electronic medical record system known as The Athletic Trainer System, which is used by many universities across the United States.[3]

27. Defendant Keffer was founded in 1994 and currently collaborates with over 600 clients across 48 states and internationally.[4] More specifically, Defendant Keffer advertises that it

[3] https://www.athletictrainersystem.com/pdf_files/Athlete_Info.pdf.
[4] https://www.athletictrainersystem.com/CompanyHistory.aspx

currently serves over 6500 schools, clinics, and other organizations with over 27,000 users and 2 million athletes.[5] Among the universities served by Keffer are Defendant University of Michigan, and Student Doe's alma mater, Grambling State University.

28. Keffer represents that its Athletic Trainer System tool was "designed with athletic trainers for athletic trainers," and is designed to store PII and PHI belonging to students including their treatment histories, diagnoses, injuries, photos, and personal details, like height and weight, mental health information, and demographic data.[6]

29. In Keffer's FAQ, it boasts that: "Keffer Development hosts all databases in our SSAE-16, SOC II and FedRamp certified data center" and that "Information security is a high priority in our company."[7] It further claims that "On top of our Data Center being FedRamp Certified, ATS is also HIPAA and FERPA compliant. We utilize a company called Compliance Helper to ensure we maintain HIPAA and FERPA compliance."[8]

30. In its Privacy Policy, Keffer acknowledges that it has obligations as a "business associate" under HIPAA: "To the extent that KDS receives or maintains patient medical information in the course of providing the Clinical EMR, that information is secured, used and disclosed only in accordance with KDS' legal obligations as a 'business associate' under HIPAA."[9]

31. Keffer's Privacy Policy further states: "KDS [Keffer] understands that storing our data in a secure manner is essential. KDS stores PII, PHI and other data using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as

[5] https://www.athletictrainersystem.com/Default.aspx
[6] *See* https://www.athletictrainersystem.com/DemoRequest.aspx
[7] https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf
[8] *Id.*
[9] https://www.athletictrainersystem.com/pdf_Files/ATS_Privacy_Policy.pdf

unauthorized use, access, disclosure, destruction or modification. Please note, however, that while KDS has endeavored to create a secure and reliable website for users, the confidentiality of any communication or material transmitted to/from the Website or via e-mail cannot be guaranteed."[10]

32. Despite recognizing these obligations, Keffer failed to implement basic, industry standard systems to protect students'—including Student Doe's—PII and PHI.

33. As one example, while Keffer maintained the option to incorporate two-factor authentication to access its Athletic Trainer System applications, it did not require that institutions and users do so.[11] A two-factor basic security measure that requires an additional layer of authentication on top of a login credential, such as a code sent via text message or email—and critically, would have prevented Defendant Weiss from gaining access to student PHI with only the access credentials belonging to other administrators and users.

34. Recent actions by the FTC, underscore the gross negligence and failings of Keffer in failing to configure its Athletic Trainer System to default to two-factor or multi-factor authentication for access to its systems containing PII and PHI. In February 2023, the FTC published an article titled, *Security Principles: Addressing underlying causes of risk in complex systems.* The article highlighted the importance of MFA, stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[12]

35. Additionally, the FTC's enforcement actions over the past five years further emphasize the critical and fundamental role MFA plays in an effective data security system, where

[10] *Id.*
[11] https://www.athletictrainersystem.com/pdf_Files/ATS_FAQ.pdf
[12] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems

the FTC has repeatedly obtained MFA as a form of injunctive relief in data security enforcement actions.[13]

36. Keffer also lacked any effective data auditing program to measure the download activity from its system, which would have allowed it to detect the massive, years-long Data Breach of its systems by University of Michigan's Coach Weiss.

B. Defendant University of Michigan and its Grossly Negligent Oversight over Defendant Weiss and Students' Private Information

37. The University of Michigan is an elite-level educational institution, with an NCAA Division I athletic program, enrolling over 900 student athletes across 29 sports.

38. In maintaining its highly regarded athletics department and program, the University of Michigan provides its student athletes with training from its elite and influential athletic coaches and professionals, including Defendant and former University of Michigan Coach Matthew Weiss.

39. The University of Michigan was grossly negligent on two fronts: (1) in its hiring and supervision of alleged sexual predator Defendant Weiss, and (2) in its hiring and oversight over Defendant Keffer and its entrusting of students' PII and PHI in the care of Defendant Keffer.

A. The University of Michigan was Grossly Negligent in its Hiring and Supervision over Defendant Weiss

40. First, in both the hiring and supervising of athletic coaches and professionals, the University of Michigan owes a duty to student athletes generally to ensure they are protected from predation by its employees and athletic staff. Its coaches and athletic staff—including Coach

[13] *E.g.*, *In re: Equifax* (July 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach; *In re Drizly* (Oct. 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million; *In re Chegg* (Oct. 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions.

Weiss—are entrusted to train, develop, and interact with young student athletes from across the country.

41. The University of Michigan was grossly negligent in its hiring of Defendant Matthew Weiss, in 2021, after Defendant Weiss had been targeting and downloading the sensitive and graphic Private Information of student athletes for *six years*.

42. The University of Michigan was also grossly negligent in its oversight of Defendant Weiss, and consciously and recklessly disregarded its duty to safeguard student athletes from alleged sexual predators, as evidenced by its failure to prevent or even detect the Data Breach perpetrated by its athletic coach Defendant Weiss, during the two years of his employ with the University of Michigan.

43. The University of Michigan was grossly negligent in its failure to investigate the Data Breach as required under state and federal law. Under Title IX, the University of Michigan must investigate all instances of sexual harassment against students, including invasions of their privacy on the basis of sex.

44. Defendant and former University of Michigan Coach Weiss preyed on and targeted women athletes during his eight-year Data Breach targeting their Private Information on the basis of their sex. By failing to protect Plaintiff's PII and PHI, inform her of the extent of the invasion, and taking all action necessary under Title IX, the University violated its obligations under Title IX. Indeed, to this day, and although the University of Michigan knew about the breach as early as January 2023, the University of Michigan has not formally informed class members impacted by Defendant and former University of Michigan Coach Weiss's predation and misconduct.

B. The University of Michigan was Negligent in Hiring/Contracting with Defendant Keffer and in Entrusting Student's PII and PHI to Keffer

45. In addition to providing coaching to its student athletes, the University of Michigan

also provides its student athletes medical treatment, including from athletic trainers employed by the University of Michigan.

46. To facilitate that treatment, the University of Michigan contracted with Keffer to use its Athletic Training System application, which required that student athletes provide the University of Michigan and Keffer with sensitive PII and PHI.

47. When collecting that information, the University of Michigan, like Keffer, accepted an obligation to protect it under contract and statutory principles, including as a "business associate" under HIPAA.

48. The University of Michigan recognizes its obligation to safeguard sensitive PII and PHI and represents in its Privacy Statement that: "The U-M recognizes the importance of maintaining the security of the information it collects and maintains, and we endeavor to protect information from unauthorized access and damage. The U-M strives to ensure reasonable security measures are in place, including physical, administrative, and technical safeguards to protect your personal information."[14]

49. Despite this obligation, the University of Michigan failed to implement the security measures needed to fulfill that promise, including staff and employee training on securing credentials, requiring multi- or two-factor authentication to use Keffer's Athletic Trainer System, overseeing third-party vendors like Keffer, in which the University of Michigan entrusted student's sensitive PII and PHI, and monitoring and auditing access to student files and Private Information.

50. In other words, the University of Michigan not only failed to ensure it had implemented sufficient security protocols and procedures across its own systems and staff, but also the University of Michigan failed to ensure Keffer had adequate security measures in place to

[14] https://umich.edu/about/privacy-statement/

protect its students' PII and PHI from theft and misuse.

51. Indeed, the University of Michigan lacked adequate training programs to detect and stop breaches like those caused by Defendant Weiss.

C. University of Michigan's Former Coach Weiss and the Data Breach

52. Because Keffer and the University of Michigan failed to implement basic, industry standard security measures, and because the University of Michigan was grossly negligent in its hiring and oversight of Defendant Weiss, together these Defendants allowed an alleged predator, ex-football coach Matthew Weiss, to access students', and in particular female student athletes', most sensitive information for nearly a decade.

53. From 2015 to 2023, Weiss gained access to student files within Keffer's Athletic Trainer System application, through compromising the passwords of a limited number of accounts with elevated access, such as the accounts of trainers and athletic directors.

54. That level of access through that number of accounts is an egregious and grossly negligent failing of data security on its face, as no institution with reasonable data security would allow such a breach over an eight-year period.

55. That access allowed Defendant Weiss to download the PII and PHI belonging to over 150,000 student athletes from over 100 institutions, including the University of Michigan and Grambling State University.

56. From there, Defendant Weiss continued his hack by downloading student athletes' passwords to access the system, using those passwords to breach their personal accounts and download personal, intimate photographs and videos that were not publicly shared. Although the athletes' passwords that Weiss downloaded were purportedly encrypted, Defendant Weiss cracked the encryption with basic internet research he conducted.

57. After cracking their passwords, through open-source research—and through information that appeared to be leaked from other data breaches—Defendant Weiss conducted additional research on targeted athletes to obtain personal information such as their mothers' maiden names, pets, places of birth, and nicknames.

58. Using the combined information that he obtained from the student athlete databases and his internet research, Defendant Weiss was able to obtain access to the social media, email and/or cloud storage accounts of more than 2,000 targeted athletes by guessing or resetting their passwords.

59. Once University of Michigan's Coach Weiss obtained access to the accounts of targeted athletes, like Student Doe, Weiss searched for and downloaded personal, intimate photographs and videos that were not publicly shared.

60. Defendant Weiss also obtained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 1,300 students and/or alumni from universities and colleges from around the country.

61. Once University of Michigan's Coach Weiss gained access to these accounts, he would search for and download personal, intimate photographs and videos.

62. In at least several instances, Defendant Weiss exploited vulnerabilities in universities' account authorization processes to gain access to the accounts of students or alumni. Weiss leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

63. The University of Michigan took no reasonable actions to oversee and ensure that coaches it hired were not intentionally and maliciously preying on student athletes and students, took no reasonable actions to prevent this access despite its duties to students, and have taken no

reasonable actions to notify or rectify harm to the victims of University of Michigan Coach Weiss's misconduct and predation.

64. To this day, and although the University knew about the breach as early as January 2023, the University has not formally informed Class Members impacted by Weiss's predation and misconduct.

65. These failings amount to gross negligence on the part of the University of Michigan.

D. Student Doe's Allegations

66. Plaintiff Student Doe is a decorated, former women's basketball player at Grambling State University.

67. While in school, Student Doe participated in the basketball program while Defendant Weiss's Data Breach was ongoing.

68. As a student athlete, Student Doe received treatment from her university's athletic trainer staff, requiring her to disclose information about her treatment, including height, weight, injuries, medications, treatment plans, and analysis on performance and recovery. To receive treatment, Student Doe was required to use the Keffer database, and the PII and PHI Student Doe disclosed was saved on Keffer's system.

69. Because Keffer never implemented the security safeguards needed to protect student Doe's PII and PHI, and because the University of Michigan was grossly negligent in its oversight of its former coach, Defendant Weiss, Defendant Weiss compromised the PII and PHI belonging to every student whose information was saved in Keffer's Athletic Trainer System database, including, on information and belief, Plaintiff's.

70. Defendant Weiss compromised all information that was saved in the Athletic

Trainer System database, including Plaintiff's treatment information, injury information, height, weight, and other highly sensitive information.

71. Student Doe received notice dated March 26, 2025 from the U.S. Department of Justice Victim Notification System that she was identified as a potential victim in the federal action against Defendant Weiss, charging him with 24 counts of unauthorized access to computers and aggravated identity theft.[15]

72. After receiving notice from the federal government that read: "If you are receiving this notification, it means that information of yours was found in possession of the defendant,"[16] Student Doe felt violated, deeply disturbed, humiliated, embarrassed, and extremely emotionally distressed; and is experiencing physical manifestations of the stress and anxiety caused by this egregious violation of her privacy—symptoms that are further exacerbated by the fact that Student Doe still has little to no information about the Data Breach.

73. This breach of information invaded Plaintiff's privacy and has devastated her personally and emotionally, as her highly sensitive Private Information was stolen by an alleged predator under circumstances that were entirely preventable by Defendant University of Michigan and Defendant Keffer.

DEFENDANTS KEFFER AND UNIVERSITY OF MICHIGAN FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS MEMBERS' PII AND PHI

74. Defendants Keffer and University of Michigan did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII and PHI it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for 150,000

[15] *See Exhibit A*.
[16]

students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

75. The FTC promulgated numerous guides which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

77. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. Defendants Keffer and University of Michigan failed to properly implement basic

[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[18] *Id.*

data security practices explained and set forth by the FTC.

79. Defendants Keffer's and University of Michigan's failure to employ reasonable and appropriate measures to protect against unauthorized access PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

80. A Data Breach such as the one Defendants Keffer and University of Michigan experienced, is also considered a breach under the HIPAA Rules because there is an unauthorized access to PHI that is not permitted under HIPAA.

81. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." 45 C.F.R. 164.40.

82. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. 45 C.F.R.164.308(a)(6).[19]

83. Defendants Keffer's and University of Michigan's Data Breach was the foreseeable consequence of a combination of insufficiencies that demonstrate that Defendants Keffer and University of Michigan failed to comply with safeguards mandated by HIPAA.

[19] *FACT SHEET: Ransomware and HIPPA*, U.S. Dept. of Health and Hum. Servs., at 4 (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

DEFENDANTS KEFFER AND UNIVERSITY OF MICHIGAN FAILED TO COMPLY WITH INDUSTRY STANDARDS

84. Defendants Keffer and University of Michigan did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for approximately 150,000 students and former students, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

85. As explained by the FBI, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[20]

86. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of cyberattacks and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no

[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 20, 2024).

users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common cyberware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

87. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different

[21] *Id.* at 3-4.

domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[22]

88. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendants Keffer and University of Michigan could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[22] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Feb. 20, 2025).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[23]

89. As described above, experts studying cyber security routinely identify medical facilities as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

90. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendants Keffer and University of Michigan, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access

[23] *See Human-Operated Ransomware Attacks: A Preventable Disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

sensitive data.

91. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

92. Given that Defendants Keffer and University of Michigan were storing the Private Information of 150,000 individuals, Defendants Keffer and University of Michigan could and should have implemented all of the above measures to prevent cyberattacks, along with the two- or multi-factor authentication discussed earlier in this Complaint.

93. The occurrence of the Data Breach indicates that Defendants Keffer and University of Michigan failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of approximately 150,000 students' and former students' PII and PHI, and ultimately leading to the exposure of highly sensitive, private, and intimate photographs and videos for 3,330 students and former students.

DEFENDANTS KEFFER AND UNIVERSITY OF MICHIGAN FAILED TO PROPERLY PROTECT PII AND PHI

94. Defendants Keffer and University of Michigan breached their obligations to Student Doe and Class Members and were otherwise grossly negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to test and assess the adequacy of its data security system;

e. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. §

164.304 definition of encryption);

p. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

q. Failing to adhere to industry standards for cybersecurity.

95. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendants Keffer and University of Michigan negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

96. Defendant University of Michigan was also grossly negligent in its failure to oversee the data security practices of third-party vendor—Keffer—in which it entrusted the sensitive private information of its students and former students.

97. Defendant University of Michigan was also grossly negligent in its hiring and oversight of Defendant Weiss, who had been perpetrating this invasion of student's privacy for 6 years before he was hired by the University of Michigan to coach its student athletes, and for 2 years of his employment by the University of Michigan where he coached and worked closely with student athletes at the University of Michigan.

98. Accordingly, as outlined below, Plaintiff and Class Members have already been severely harmed by this egregious violation of their privacy by Defendant Weiss.

CLASS ALLEGATIONS

99. Student Doe brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

100. The Class that Student Doe seeks to represent is defined as follows:

> All individuals in the United States whose Private Information was actually or potentially accessed or acquired during the Data Breach,

("Nationwide Class" or "Class").

101. Excluded from the Class are Defendants' officers and directors; any entity in which any Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of any Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

102. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. The U.S. Department of Justice has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, has already sent preliminary notice to affected individuals, including Plaintiff.

103. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants Keefer and University of Michigan failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the hacking incident and Data Breach;

c. Whether Defendants Keefer and University of Michigan data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, FTC Guidelines, HIPAA, etc.;

d. Whether Defendants Keefer's and University of Michigan's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants Keefer and University of Michigan owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendants Keefer and University of Michigan breached their duty to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether Defendant University of Michigan was grossly negligent in its

hiring and supervision of Defendant Weiss;

h. Whether Defendant University of Michigan was grossly negligent in its oversight of Defendant Keefer;

i. Whether Defendants Keefer and University of Michigan knew or should have known that their data security systems and monitoring processes were deficient;

j. Whether Defendants Keefer and University of Michigan owed a duty to provide Plaintiff and Class Members timely notice of the Data Breach, and whether Defendants Keefer and University of Michigan breached that duty to provide timely notice;

k. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

l. Whether Defendants' conduct was negligent or grossly negligent;

m. Whether Defendant's conduct was *per se* negligent;

n. Whether Defendants' conduct violated federal laws;

o. Whether Defendants' conduct violated state laws; and

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages.

104. Common sources of evidence may also be used to demonstrate Defendants' unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

105. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach and Defendants' misfeasance.

106. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent

and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

107. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendants engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way and as a result of the same vulnerabilities. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants Keefer and University of Michigan. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

109. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Members to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

110. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

111. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

112. Unless a class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

113. Further, Defendants acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

114. Defendants acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

115. Finally, all members of the proposed Class are readily ascertainable. The U.S. Department of Justice has identified hundreds of thousands of individuals whose Private Information may have been improperly accessed in the Data Breach and has already sent preliminary notice to affected individuals, including Plaintiff.

CAUSES OF ACTION

FIRST COUNT
Negligence & Negligence *Per Se* Against Keffer Only
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

117. Plaintiff brings this claim individually and on behalf of Class Members.

118. Plaintiff and Class Members entrusted their PII and PHI to Keffer. Keffer owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

119. Plaintiff and Class Members entrusted their Private Information to Keffer on the premise and with the understanding that Defendant Keffer would safeguard their information, use their PII and PHI for purposes that would benefit Plaintiffs and Class Members and/or not disclose their PII and PHI to unauthorized third parties.

120. Defendant Keffer owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Keffer's failure to adequately safeguard their PII and PHI in accordance

with industry standards concerning data security would result in the compromise of that PII and PHI—as occurred in the Data Breach.

121. Defendant Keffer acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII and PHI by misrepresenting their commitments to high standards of security in their public representations on their website, when in reality their lack of security allowed Plaintiff's and Class Members' PII and PHI to be accessed and exfiltrated by malicious actors including Defendant Weiss.

122. Defendant Keffer further breached its duty of care to Plaintiff and Class Members by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for ensuring the reasonable and adequate security of that PII and PHI.

123. Defendant Keffer had full knowledge of the sensitive nature of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII and PHI was wrongfully disclosed.

124. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant Keffer's security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendant Keffer's possession was adequately secured and protected.

125. Defendant Keffer had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within their possession was compromised and precisely the type(s) of information that were compromised.

126. Defendant Keffer had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

127. Defendant Keffer owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Keffer also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the breach.

128. Defendant Keffer owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Keffer knew or should have known would suffer injury-in-fact from Defendant Keffer's inadequate security protocols. Keffer actively sought and obtained Plaintiff's and Class Members' PII and PHI.

129. The risk that unauthorized persons would attempt to gain access to the PII and PHI in Defendant Keffer's care, and misuse it was foreseeable. Given that Defendant Keffer holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Keffer's databases containing the PII and PHI.

130. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPAA and/or Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

131. These regulations were intended to protect the Class at issue here, and Keffer's failure to abide by them caused Plaintiff and the Class damages.

132. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is

properly maintained.

133. Defendant Keffer's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Keffer and Class Members, which is recognized by laws and regulations, as well as common law. Defendant Keffer was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach and was considered a "business associate" under HIPAA.

134. In addition, Defendant Keffer had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Defendant Keffer's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

136. Defendant Keffer systematically failed to provide adequate security for data in its possession.

137. Defendant Keffer was subject to an "independent duty," untethered to any contract between Defendant Keffer and Plaintiff or Class Members.

138. The specific negligent acts and omissions committed by Defendant Keffer include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' PII and PHI;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's Class Members' PII And PHI, including, but not limited to, its failure to require two- or multi-factor authentication for access to its Athletic Trainer System;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards and detect an unauthorized access;

e. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2)

g. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

h. Failing to ensure compliance with HIPAA security standards under 45 C.F.R. § 164.306(a)(4);

i. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

j. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1); and

k. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

139. Defendant Keffer, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within Defendant Keffer's possession.

140. Defendant Keffer, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

141. Defendant Keffer, through its actions and/or omissions, unlawfully breached its

duty to timely disclose to Plaintiff and Class Members that the PII and PHI within Defendant Keffer's possession might have been compromised and precisely the type of information compromised.

142. It was foreseeable that Defendant Keffer's failure to use reasonable measures to protect Plaintiff and Class Members' PII and PHI would result in injury to Plaintiff and Class Members.

143. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII and PHI would result in injuries to Plaintiff and Class Members.

144. Defendant Keffer's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

145. Keffer's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

146. Defendant's breaches of duties caused Plaintiff and Class Members to suffer from identity theft, invasion of privacy, severe emotional distress, loss of dignity, and embarrassment, and other physical and mental harm.

147. As a result of Defendant Keffer's negligence and breaches of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, including predator Defendant Weiss, will be used for malicious and deviant purposes.

SECOND COUNT
Negligent Hiring and Supervision and Gross Negligence Against University of Michigan Only
(On Behalf of Plaintiff and the Nationwide Class)

148. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

a. Negligent Supervision over Defendant Keffer

149. At all relevant times, Keffer was the University of Michigan's agent. University of Michigan granted Keffer access to Plaintiff's and Class Members' PII And PHI without properly:

a. Vetting Keffer;

b. Inquiring about, investigating, or monitoring Keffer's data security practices;

c. Training Keffer;

d. Advising Keffer of the duties owed to Plaintiff and Class Members; or

e. Advising Keffer of the confidential nature of Plaintiff's and Class Members PII and PHI.

150. The University of Michigan was negligent and failed to exercise care in the hiring, supervision, and retention of Keffer – whose inadequate data security, training, procedures, protocols, and network infrastructure led to the Data Breach and caused the damages suffered by Plaintiff and Class Members, as alleged herein.

151. At all times relevant hereto, University of Michigan owed a duty to Plaintiff and Class Members to train and supervise its agents, vendors, and third parties handling sensitive student data in its possession and control, and to ensure they recognized the duties owed to Plaintiff and Class Members to keep their PII and PHI safe from unauthorized access and disclosure.

152. The University of Michigan owed a duty to Plaintiff and Class Members to ensure Keffer had adequate data security procedures and practices sufficient to protect Plaintiff's and

Class Members' PII and PHI, prior to hiring or contracting with Keffer.

153. After hiring or contracting with Keffer, the University of Michigan also owed a continuing duty to Plaintiff and Class Members to ensure Keffer continued to employ adequate data security procedures and practices to protect Plaintiff's and Class Members' PII and PHI from unauthorized access or disclosure.

154. The University of Michigan was on notice of the importance of data security because of previous highly publicized data breaches affecting HIPAA business associates and PHI.

155. Despite being aware of this risk, University of Michigan failed to ensure that Keffer employed adequate data security measures to protect Plaintiff's and Class Members' PII and PHI from unauthorized disclosure and access by parties with criminal, malicious, and predatory intent.

156. The University of Michigan knew or should have known that its failure to ensure that Keffer employed adequate data security measures would create a foreseeable and unreasonable risk of harm to Plaintiff and Class Members.

157. As a direct and proximate result of the University of Michigan's breach of its duties, and their negligent hiring, training, and supervision of Keffer, Plaintiffs' and Class Members' PII and PHI were compromised and stolen in the Data Breach.

b. Grossly Negligent Hiring and Supervision as to Defendant Weiss

158. Between 2021 and 2023, University of Michigan's Coach Matthew Weiss was the employee and agent of Defendant University of Michigan.

159. The University of Michigan owed a duty of care to Class Members to use reasonable care in hiring and retaining only those employees who would not cause Class Members to suffer injury.

160. During this time, University of Michigan granted Weiss access to Class Members

and to Plaintiff's and Class Members' Private Information without properly:

a. Vetting Weiss;

b. Inquiring about, investigating, or monitoring Weiss's data security practices and computer use;

c. Perceiving, understanding, and preventing inappropriate sexual harassment on campus;

d. Perceiving, reporting, and preventing inappropriate invasion of privacy campus;

e. Providing diligent supervision to and over student athletes and other individuals, including Defendant Weiss;

f. Thoroughly investigating any invasion of privacy by Defendant Weiss;

g. Ensuring the safety of all students, faculty, staff, and visitors to the University of Michigan's campuses and premises;

h. Providing a safe environment for all students, faculty, staff, and visitors to the University of Michigan's premises free from sexual harassment; and

i. Properly training faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment.

161. The University of Michigan was negligent and failed to exercise care in the hiring, supervision, and retention of Weiss – whose inappropriate, unlawful, and highly invasive and offensive conduct led to the Data Breach and caused the damages suffered by Plaintiff and Class Members, as alleged herein.

162. At all times relevant hereto, University of Michigan owed a duty to Plaintiff and Class Members to train and supervise its agents, employees, and athletic staff and coaches—including Defendant Weiss—while he was in the course of his employment, agency and/or

representation of the University of Michigan and while he interacted with young female students, handled sensitive student data in the University of Michigan's control and possession and control, and was in close proximity to students to ensure they recognized the duties owed to Plaintiff and Class Members to not abuse them.

163. Defendant Weiss's unlawful Data Breach started years before University of Michigan hired Defendant Weiss to serve as a coach to its student athletes, and yet University of Michigan failed to perform a reasonable background check or take other reasonable and adequate pre-hiring precautions to ensure that its employees did not have malicious, criminal, or inappropriate intentions towards students.

164. It was reasonably foreseeable given the *6 years* of Defendant Weiss's hacking and harassment of students and student athletes that preceded his hiring by the University of Michigan that he would continue his unlawful and egregious invasion of students' privacy, unless properly supervised.

165. The University of Michigan failed to investigate, or adequately investigate, or was grossly negligent in investigating Defendant Weiss's background and misconduct towards students and student athletes.

166. The University of Michigan knew or should have known that its failure to ensure that Defendant Weiss did not have malicious, criminal, or inappropriate intentions towards students would cause a foreseeable and unreasonable risk of harm to Plaintiff and Class Members.

167. The University of Michigan knew, or by the exercise of diligence and reasonable care should have known, that Weiss was improperly searching for, accessing, inspecting, downloading, exporting, and stealing Plaintiff's and Class Members Private Information.

168. It was reasonably foreseeable given Defendant Weiss's six-year-long history of

harassing actions toward students and student athletes that he would continue his pattern of abuse of students, including Plaintiff and Class Members, unless properly supervised.

169. The University of Michigan controlled Weiss's coaching, his hours, his company computer and network access, and his authorization for access to Keffer's systems and databases. The University of Michigan had the ability and duty to monitor Weiss's searches, views, downloads, uploads, and other activities involving these systems, databases, and student data. Yet University of Michigan either (a) monitored those activities, yet did nothing to stop them, or (b) willingly chose not to monitor those activities. University of Michigan thus breached its duty reasonably to supervise or monitor its employees and stop any unauthorized inspection or disclosure of confidential and sensitive Private Information and was grossly negligent in so doing.

170. The University of Michigan was grossly negligent in permitting its employees, including Defendant Weiss, to use its computers, computer networks, or credentials to access the Private Information Plaintiff and Class Members.

171. The Data Breach occurred while Defendant Weiss was acting in the course of his employment, agency and/or representation of the University of Michigan.

172. University of Michigan's hiring and supervision over Defendant Weiss was so reckless as to demonstrate a substantial lack of concern for whether injury would result to Plaintiff and Class Members.

173. University of Michigan's hiring and supervision over Defendant Weiss was substantially more than negligent.

174. As a direct and proximate result of the University of Michigan's breach of its duties, and their negligent hiring, training, and supervision of Weiss, Plaintiffs' and Class Members' Private Information was compromised and stolen in the Data Breach.

175. The University of Michigan tolerated, authorized and/or permitted a custom, policy, practice or procedure of insufficient supervision and failed to adequately screen, counsel or discipline Defendant Weiss, with the result that Defendant Weiss was allowed to violate the rights of persons such as Plaintiff and Class Members with impunity.

176. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

177. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

THIRD COUNT
Breach of Implied Contract Against Keffer Only
(On Behalf of Plaintiff and the Nationwide Class)

178. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

179. Defendant Keffer, as a condition of providing its services, required Plaintiff and Class Members to provide and entrust their PII and PHI.

180. By Plaintiff and Class Members providing their PII and PHI to Defendant Keffer, and by Defendant Keffer accepting this PII and PHI and representing it would maintain the safety and security of this PII and PHI, including through its privacy policies, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant Keffer would adequately safeguard Plaintiff's and Class Members' PII and PHI from foreseeable threats, (2) that Defendant Keffer would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant Keffer would provide Plaintiff and Class Members with notice within a reasonable

amount of time after suffering a data breach.

181. Defendant Keffer provided consideration by providing its services, while Plaintiff and Class Members provided consideration by paying for its services, either directly or indirectly through their enrollment at educational institutions, and providing valuable property—*i.e.*, their PII and PHI—to Defendant Keffer. Defendant Keffer benefitted from the receipt of this PII and PHI by increased income through providing its Athletic Trainer Software.

182. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant Keffer.

183. Defendant Keffer breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and PHI or providing timely and accurate notice to them that their PII and PHI was compromised due to the Data Breach.

184. Defendant Keffer's breaches actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

FOURTH COUNT
Unjust Enrichment against Keffer Only
(On Behalf of Plaintiff and the Nationwide Class)

185. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

186. Plaintiff pleads this Count in the alternative to her Implied Contract claim.

187. Plaintiff and Class Members conferred a monetary benefit on Defendant Keffer, either directly or indirectly through their educational institutions, by providing Defendant with payment for its services and with valuable PII and PHI in exchange for the use of Keffer's Athletic Trainer System software

188. Defendant Keffer enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI.

189. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant Keffer instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

190. Under the principles of equity and good conscience, Defendant Keffer should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant Keffer failed to implement appropriate data management and security measures that are mandated by industry standards.

191. Defendant Keffer acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

192. If Plaintiff and Class Members knew that Defendant Keffer had not secured their PII and PHI, they would not have consented to provide it to Defendant Keffer, either directly or indirectly.

193. Plaintiff and Class Members have no adequate remedy at law.

194. Defendant Keffer actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

195. As a direct and proximate result of Defendant Keffer's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

196. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

FIFTH COUNT
Invasion of Privacy: Intrusion Upon Seclusion
Against Defendant Weiss Only
(On Behalf of Plaintiff and the Nationwide Class)

197. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

198. Plaintiff and the Class's Private Information was stored electronically and was intended to remain private.

199. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant Weiss hacked, accessed, viewed, exfiltrated, and kept detailed personal notes on.

200. Defendant Weiss unlawfully and intentionally accessed this private and personal information, invading on the seclusion and private affairs of Plaintiff and Class Members.

201. Defendant Weiss's actions were unauthorized, and the invasion would be highly offensive to any reasonable person.

202. A reasonable person of ordinary sensibilities would consider the viewing of Plaintiff's and Class Members' Private Information by an unauthorized person to be highly offensive.

203. Plaintiff and the Class never granted permission for this access and Defendant Weiss's intrusion is a severe violation of their privacy, causing them severe emotional damages.

204. Defendant Weiss actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, which injury-in-fact and damages are ongoing,

imminent, immediate, and which they continue to face.

205. Plaintiffs and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

SIXTH COUNT
Violation of the Civil Rights Act: Failure to Train and Supervise
Against only the University of Michigan
42 U.S.C. § 1983
(On Behalf of Plaintiff and the Nationwide Class)

206. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

207. The University of Michigan had the ultimate responsibility and authority to train and supervise its employees, agents, and/or representatives including Defendant Weiss and all faculty and staff regarding their duties toward students, faculty, staff and visitors.

208. The University of Michigan failed to train and supervise its employees, agents, and/or representatives including all faculty and staff, regarding the following duties:

a. Perceiving, understanding, and preventing inappropriate sexual harassment on campus;

b. Perceiving, reporting, and preventing inappropriate invasion of privacy on campus;

c. Providing diligent supervision to and over student athletes and other individuals, including Defendant Weiss;

d. Thoroughly investigating any invasion of privacy by Defendant Weiss;

e. Ensuring the safety of all students, faculty, staff, and visitors to the University of Michigan's campuses and premises;

f. Providing a safe environment for all students, faculty, staff, and visitors to the University of Michigan's premises free from sexual harassment; and

g. Properly training faculty and staff to be aware of their individual responsibility for creating and maintaining a safe environment

209. The University of Michigan failed to adequately train coaches, trainers, medical staff, Weiss, and others regarding the duties listed above which led to violations of Plaintiff's and Class Members' rights

210. The University of Michigan's failure to adequately train was the result of its deliberate indifference toward the well-being of student athletes.

211. As a result, the University of Michigan deprived Plaintiff and Class Members of rights secured by the Fourteenth Amendment to the United States Constitution in violation of 42 U.S.C. § 1983.

212. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress— which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

213. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

SEVENTH COUNT
Violation of the Civil Rights Act: State Created Danger
Against only the University of Michigan
42 U.S.C. § 1983
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

215. The due process clause of the 14th Amendment provides that the state may not deprive a person of life, liberty or property without due process of law.

216. The University of Michigan recklessly exposed Plaintiff to a dangerous alleged predator, Defendant Weiss, knowing he could cause serious damage by sexually harassing female students, and also by violating their rights to privacy.

217. In hiring Defendant Weiss, six years into his scheme to invade the privacy of female students, University of Michigan took an affirmative action that increased the risk that Plaintiff and Class Members would be exposed to harm by the misconduct and unlawful acts of Defendant Weiss.

218. In putting Defendant Weiss in a coaching position at the University of Michigan, a position of power with easy access to student athletes and female students, University of Michigan placed Plaintiff and Class Members—all students and student athletes—specifically at risk.

219. The University of Michigan knew or should have known that hiring an alleged sexual predator—Defendant Weiss—would specifically endanger Plaintiff and Class Members.

220. Plaintiff, as a female student athlete was a foreseeable victim.

221. The invasion of Plaintiff's and Class Members privacy was foreseeable. The decisions and actions to deprive Plaintiff and Class Members of a safe educational experience constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff and Class Members.

222. The University of Michigan acted in willful disregard for the safety of Plaintiff and Class Members, or the University of Michigan was grossly negligent and wantonly reckless in its disregard for the safety of Plaintiff and Class Members.

223. The decisions and actions to deprive Plaintiff and Class Members a safe college experience constituted affirmative acts that caused and/or increased the risk of harm, as well as physical and emotional injury, to Plaintiff.

224. Defendant University of Michigan actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress— which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

225. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

EIGTH COUNT
Violation of the Stored Communications Act
Against Only Defendants University of Michigan and Weiss
18 U.S.C. § 2701 *et seq*
(On Behalf of Plaintiff and the Nationwide Class)

226. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

227. The Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits the intentional access of web-based cloud storage and media accounts, including email or other online databases (including Keffer's Athletic Trainer System), that contain personal, private, and intimate information.

228. Any person who intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided 18 U.S.C. § 2701(b).

229. Plaintiff's and Class Members' electronic information and communications were in electronic storage and fit directly within the protections of the statute. The information, messages, files, and media were accessed by Defendant Weiss without authorization, in part, and

over the course of two years, in connection with his employment with the University of Michigan.

230. Weiss's access without authorization, in part, in connection with his University of Michigan job duties as an athletic coach were intentional and knowingly perpetrated.

231. Defendant Weiss's access to Keffer and to other sources of students stored communications were heightened and supported by his status as an employee of the University of Michigan, working in the capacity of an athletic trainer and coach hired by the University of Michigan, with access to Keffer's Athletic Trainer System.

232. Because Defendant Weiss violated the Stored Communications Act within the scope of his employment as an athletic trainer and Coach at the University of Michigan—which gave him high level security access to Keffer's database of student PHI and PII—the University of Michigan is also liable for the actions of Defendant Weiss to violate the Stored Communications Act.

233. The University of Michigan is vicariously liable for Defendant Weiss's actions because he committed these actions in furtherance of his role as an employee of the University of Michigan. The University of Michigan is liable for completed offenses carried out by Defendant Weiss.

234. Plaintiff and Class Members may assert a claim under § 2707 of the Stored Communications Act, for which there is strict liability.

235. The Stored Communications Act provides that a person aggrieved by a violation of the act may seek appropriate relief including equitable and declaratory relief, actual damages or damages no less than $1,000, punitive damages, and reasonable attorney's fee[s] and other litigation costs reasonably incurred according to 18 U.S.C. § 2707(b)-(c).

236. Defendant Weiss's access to Plaintiff's and Class Members' private, personal, and

intimate information, messages, files, and media was in violation of 18 U.S.C. § 2701(a). As described above, the University of Michigan is also liable for this access which was, for two years, perpetrated in the scope of his employment by the University of Michigan.

237. Defendant Weiss knew he did not have authority to access Plaintiff's and Class Members' private, personal, and intimate information, messages, files, and media but accessed them nevertheless with intentionality.

238. Under the statute, Plaintiff and Class Members should be granted the greater of (1) the sum of their actual damages suffered as a result of the violations or (2) $1,000 per violation of the Stored Communications Act.

239. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach, and attorneys' fees and costs.

NINTH COUNT
Violation of the Computer Fraud and Abuse Act
Against Only Defendants University of Michigan Weiss
18 U.S.C. § 1030, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

240. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein

241. Defendant Weiss violated the Computer Fraud and Abuse Act ("CFAA") by unlawfully accessing Plaintiff's private information without authorization.

242. Defendant Weiss did so in the course of his assigned job responsibilities at the University of Michigan where he worked as a trainer and Coach and therefore was provided with heightened access to Keffer's Athletic Trainer System by the University of Michigan.

243. Defendant Weiss's actions constitute a violation of the Act because he "knowingly accessed a computer without authorization" and/or "exceeded authorized access, thereby

obtaining... information." 18 U.S.C. § 1030(a)(2)(C).

244. Under the CFAA, Defendant Weiss surpassed the scope of his permitted access by entering restricted areas of the digital network and exfiltrating sensitive PHI and PII of students for which he was not authorized to access or download.

245. As described above, Defendant Weiss's actions were intentional, as he exploited Keffer's and the University of Michigan's security failures to prey on students.

246. The University of Michigan is vicariously liable for his actions because he committed these actions in furtherance of his role as an employee of the University. The University of Michigan is liable for completed offenses carried out by Defendant Weiss.

247. Under 18 U.S.C. § 1030(g), Plaintiff and Class Members may recover damages in this civil action from Defendant Weiss and the University of Michigan along with injunctive relief or other equitable relief.

248. Defendants University of Michigan and Weiss actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages—including humiliation, embarrassment, loss of dignity, and severe emotional distress— which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

249. Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and Plaintiff's counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

Dated: April 8, 2025

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

James J. Pizzirusso
Amanda V. Boltax*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
T: 202.540.7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com

Steven M. Nathan
Ashley M. Crooks*
HAUSFELD LLP
33 Whitehall Street 14th Floor
New York, New York 10004
T: 646.357.1100
acrooks@hausfeld.com

Counsel for Student Doe

**Application for Pro Hac Vice forthcoming*